

Università degli Studi di Bologna
DEIS

WPA-GPG: Wireless authentication using GPG Key

Gabriele Monti

December 9, 2009

WPA-GPG: Wireless authentication using GPG Key

Gabriele Monti¹

¹*DEIS - University of Bologna*
Via Venezia, 52
Cesena I-47023
gabriele.monti4@unibo.it

December 9, 2009

Abstract. In this paper we present WPA-GPG, a modification on WPA-PSK wireless authentication protocol that allows a wireless station to access a protected network using a GnuPG public key. GnuPG, (GPG) short for GnU Privacy Guard, is a complete, multi-platform and open source implementation of the OpenPGP standard as defined by RFC4880. Like WPA-PSK, WPA-GPG is based on IEEE802.1X and EAP protocols, therefore it does not require any special hardware to work, any wireless card supporting IEEE 802.11i (WPA2) standard is suitable for WPA-GPG. Differently from WPA-PSK, WPA-GPG ensures in-network users' privacy and non-repudiation of network traffic.

Keywords: *wireless, authentication, WPA2, GPG*

Contents

1	Introduction	3
2	Related works	3
3	WPA-GPG: Modified four-way handshake protocol	5
3.1	Message 1/4	7
3.2	Message 2/4	8
3.3	Message 3/4	9
3.4	Message 4/4	9
4	Conclusions	10

1 Introduction

WPA-GPG is a modification on WPA-PSK authentication protocol that allows a wireless station (also known as supplicant or STA) to gain access to a protected wireless network, managed by an Access Point (also known as AP or authenticator), by means of its personal GPG key. GnuPG [1], short for GnU Privacy Guard, is a complete and open source implementation of the OpenPGP standard as defined by RFC4880. GnuPG allows to manage keys, encrypt and sign data and communication, it is a mature and robust project and we believe that its multi-platform support may facilitate the adoption of WPA-GPG. Currently, WPA-GPG verifies that the authenticating STA is the owner of the key that it is providing to the AP, this represents the core of the authentication process. Future development works will be done to allow the AP to verify that the provided key belongs to a specific key list (ACL style) or even to query a GPG key-server to check if the key has been signed by a trusted key (network of trust style). The former authentication mode could be more suitable in a domestic environment while the latter could be employed to create a community of users willing to share their connectivity (an example of such a community is Fon[2]) or for public administrations to provide public Wi-Fi access. WPA-GPG does not require specific hardware nor firmware since, as we will show in the next pages, its modifications to the original protocol are important but not radical. WPA-GPG ensures the same level of security of WPA-PSK but it also guarantees in-network user privacy and non-repudiation of network traffic. With the term *in-network user privacy* we mean that network traffic is crypted in a way that even STAs which have the right to authenticate are not able to decrypt it. As we will show this is not possible in WPA-PSK. As a direct consequence WPA-GPG also allows the AP to know exactly which STA has generated what traffic, ensuring non-repudiation.

The paper is organized as follows, in Section2 we discuss some issues regarding WPA-PSK authentication with respect to our protocol. In Section 3 we present our modified authentication protocol and in Section4 we summarize our contribution.

2 Related works

IEEE 802.11i (also known as WPA2) is a standard developed by IEEE to provide a security layer to (wireless) communications based on IEEE 802.11 standard. WPA2 defines specifications regarding all of the main aspects involved in wireless networks security:

- Management of STAs associations;
- Authentication protocol;

Field	Length in octets
Element ID	1
Element Length	1
Version	2
Group key suite	4
Pairwise suite count	2
Pairwise suite list	4 per pairwise suite
Authentication suite count	2
Authentication suite list	4 per authentication suite
Capabilities	2

Table 1. *IE RSN message structure.*

- Session Key management.

Management of STAs associations. WPA2 uses RSN (Robust Secure Network) protocol to manage STA associations. RSN require STA and AP to exchange information regarding authentication and cypher capabilities, namely the supported authentication and key management protocols. This exchange allows STA and AP to agree about the most robust and secure protocols among the available ones. Information exchanged is achieved by using Information Elements (IE) messages whose format is defined within RSN protocol. In Table 1 we show the structure of IE RSN messages.

An observation of the IE structure makes clear the fact that both AP and STA may be able to authenticate using different protocols. When this is the case it could be possible for an attacker to try a *version rollback attack* by forging association messages and forcing AP and STA to use the weaker protocol among the available ones. As we will see, WPA-PSK is implemented in such a way that both STA and AP can check that they're agreeing on a non-forged RSN IE and therefore they are using the most secure available protocols. WPA-GPG guarantees this feature as well.

Authentication protocol. WPA-PSK authentication protocol uses EAPOL messages, whose format is defined within the Extensible Authentication Protocol (EAP), but it reduces to a four-way handshake aiming to verify that STA knows the secret Pre-Shared Key, also known as Pairwise Master Key (PMK), and to establish a Pairwise Transient Key (PTK) which is installed into the MAC layer. A PTK is generated in order to reduce as much as possible the use of PMK and, as a consequence, its exposition to attacks. Besides PTK a Group Transient Key (GTK) is generated to allow the transmission of multicast and broadcast traffic within the wireless network. The PSK is 256 bit long and can be set through a passphrase, namely an alphanumeric sequence which is then hashed to obtain the PSK, or di-

rectly as 64 characters long hexadecimal string. After a successful 4-Way Handshake, a secure communication channel between the authenticator and the supplicant can be constructed for subsequent data transmissions, based on the shared PTK and/or GTK. The 4-Way Handshake may be repeated using the same PMK. The PTK is derived from a hashing function applied to a combination of the PMK, the STA and AP MAC addresses and two 32 byte long random numbers generated by STA and AP called Snonce and ANonce respectively. We can make two consideration regarding WPA-PSK security. The first, although there is no design flaw in WPA-PSK, the way it is used and implemented make it vulnerable. In fact, people are usually brought to choose short passphrases as their shared secrets. Since the four messages of four-way handshake must be transmitted in clear-text an observer is able to read STA and AP MAC addresses as well as both Snonce and ANonce, if the chosen passphrase is weak dictionary based attacks or a brute force attack are possible. The second consideration regards communication privacy within the network since any subject which knows the PSK is able to sniff others communications across the network. Although this can not be considered as a flaw we believe privacy is a plus for an authentication protocol. WPA-GPG solve the problem of weak passphrases and by exploiting public-key cryptography properties allows in-network privacy as well as non-repudiation of traffic.

The whole four-way handshake protocol is run in a 802.1X controlled environment. 802.1x is an IEEE Standard for port-based Network Access Control (PNAC), adopted in WPA2, in which “port” means a single point of attachment to the network infrastructure. After a successful association, which corresponds to “authorized state” in 802.1X, STA and AP have opened a (logical) “controlled port” through which only 802.1X ethernet frames are allowed. EAPOL messages used during four-way handshake are encapsulated in 802.1X frames and therefore allowed. After successful authentication STA and AP can open the “uncontrolled port” through which any kind of traffic is allowed. WPA-GPG does not modify any aspect regarding association and 802.1X with respect to WPA-PSK.

Session Key management. WPA2 introduced CCMP, a key management protocol designed to be more robust with respect to its predecessor TKIP which was earlier introduced as a temporary replacement to WEP and which could work without requiring new hardware capabilities.

3 WPA-GPG: Modified four-way handshake protocol

As reported in the previous section the goal of WPA-PSK four-way handshake protocol is to create a PTK known both to supplicant and authenticator while not revealing the PMK. WPA-GPG has exactly the same goal, with the difference that no PSK is shared between STA and AP but STA uses its GPG key to authenticate. In WPA-GPG the PMK is randomly generated by the AP, crypted and sent to the

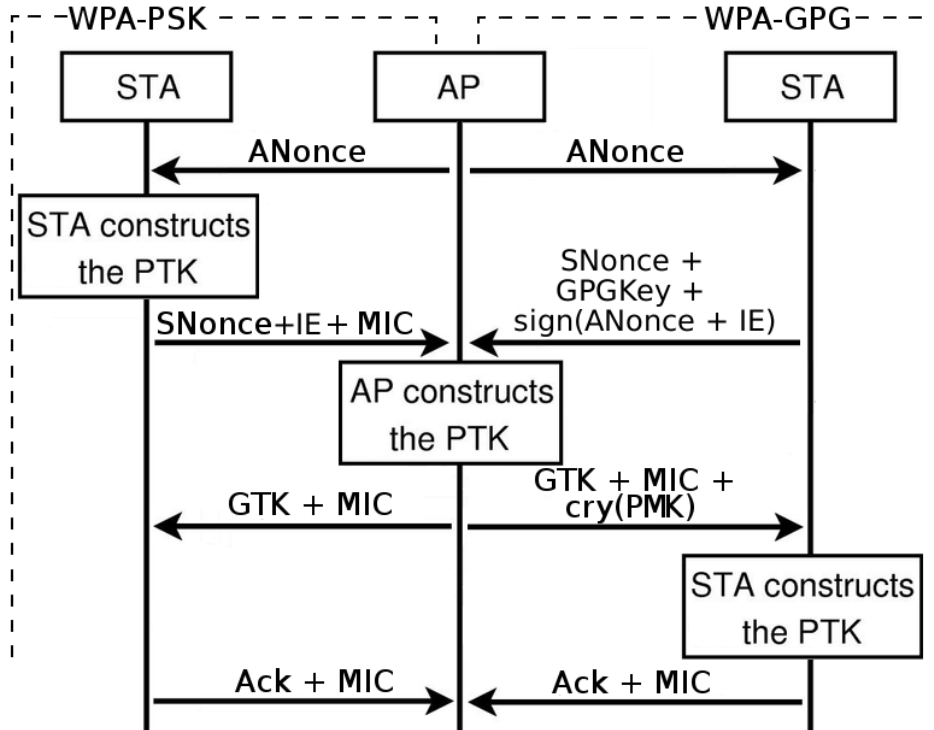


Figure 1. Comparison between WPA-PSK and WPA-GPG four-way handshake protocols.

authenticating STA. Both AP and STA will therefore be able to derive a PTK from the PMK, exactly as it happens with WPA-PSK, with the main difference that each PTK can not be derived by other STAs.

Figure 1 shows the differences between the two protocols.

Before using the protocol AP and STA must agree about using WPA-GPG. In order to achieve that we added a constant flag (10th bit enabled) on the *Capabilities* field of RSN IE. Table 2 shows an example of RSN IE with WPA-GPG enabled.

Capabilities value must be converted in big endian representation, obtaining 10000000000 in binary form.

The handshake protocol is performed using EAPOL Key messages. Message format is shown in Table 3. WPA-GPG extends the original message format by adding a field containing the size of GPG extra payload and another field representing the payload itself. For each message we will describe the extra payload.

Other fields have the same meaning as intended in WPA-PSK. For instance the field *emphkey_info* contains information regarding the key itself, type, version, if it is crypted or not, if MIC is included or not, etc. MIC means Message Integrity Code,

Field	Value
Element ID	30
Element Length	14 (20)
Version	01 00
Group key suite	00 0f ac 04
Pairwise suite count	01 00
Pairwise suite 1	00 0f ac 04
Authentication suite count	01 00
Authentication suite 1	00 0f ac 02
Capabilities	00 04

Table 2. *RSN IE transmitted by AP with WPA-GPG enabled.*

Field	Length in octets
type	1
key_info	2
key_length	2
replay_counter	8
key_nonce	32
key_iv	16
key_rsc	8
key_id	8
key_mic	16
key_data_length	2
key_data_length bytes of key data	
wpa_gpg_data_length	2
wpa_gpg_data_length bytes of WPA-GPG data	

Table 3. *EAPOL key structure.*

it is a digest of the message content obtained using part of the PTK as key, it is useful to verify the message integrity and protect it to external attacks.

3.1 Message 1/4

The first message is sent by the AP and contains the same informations in both WPA-PSK and WPA-GPG, namely the AP random nonce (*ANonce*). This message is not crypted and no MIC is attached (the PTK cannot be derived yet).

Field	Valore
type	02
key_info	40 0a
key_length	00 00
replay_counter	00 00 00 00 00 00 00 01
key_nonce	6d 6d 36 e3 28 42 ab cc 24 95 ad ce 57 bb 54 08 bc 1d 12 65 ba 38 c8 2f 23 9b 46 5e 0a 81 66 9e
key_iv	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
key_rsc	00 00 00 00 00 00 00 00
key_id	00 00 00 00 00 00 00 00
key_mic	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
key_data_length	00 16
key_data	30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 00 04
wpa_gpg_data_length	00 80
wpa_gpg_data	59 6f c5 1f 5a bd e8 c3 2d c6 a4 59 ae d9 7a 08 83 12 fd 3c a8 63 0c 57 31 40
wpa_gpg_data_length	00 80
wpa_gpg_data	a9 09 b9 6f 77 23 b7 5c e9 5e b1 9f 39 d0 c5 51 c8 67 aa aa 1c 86 02 15 79 89
wpa_gpg_data_length	00 01
wpa_gpg_data	29

Table 4. Example of 2/4 message, protocol WPA-GPG.

3.2 Message 2/4

In WPA-PSK, upon receiving message 1 of 4 and having generated its random nonce (*SNonce*) STA knows all the information required to derive PTK from PMK. On the other side, in WPA-GPG no PMK is available yet, therefore WPA-GPG message 2 of 4 will contain no MIC information. However message 2 of 4 will contain some WPA-GPG specific data (see Table 4):

- Signature of ANonce and received RSN IE;
- STA Public key.

Besides these information STA will attach its nonce and the RSN IE received.

The signed RSN IE is added to allow AP to verify that the STA has received a correct element and to prevent *version rollback attacks*. In WPA-PSK the correctness of IE is checked through MIC verification.

3.3 Message 3/4

In WPA-PSK, on reception of message 3 of 4 AP is able to derive PTK, check MIC correctness and continue the authentication by attaching GTK in message 3 of 4. In WPA-GPG AP performs different tasks for message preparation (see Table 5):

- Verifies the validity of STA signature on *ANonce*, using the key attached to message 2 of 4;
- Generates a random 32 byte PMK and derives the PTK;
- Attaches IE and GTK to the message and computes message MIC;
- Crypt the generated PMK using STA public key.

Field	Valore
type	02
key_info	53 ca
key_length	00 10
replay_counter	00 00 00 00 00 00 00 02
key_nonce	06 7b f0 18 7e 9d af 94 35 95 0f 8b b5 90 6b ab 4d 6d b0 27 cf d9 eb d6 3e f6 ae 10 9a 47 be 96
key_iv	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
key_rsc	07 00 00 00 00 00 00 00
key_id	00 00 00 00 00 00 00 00
key_mic	73 ac d9 ab b8 3c 1b f2 47 04 68 cf bd 93 b5 16
key_data_length	00 38
key_data	ba c9 74 61 1c c9 15 d9 f0 ce 51 f5 2b 92 fc 90 fa 21 93 52 39 f4 b0 18 89 d4
wpa_gpg_data_length	00 7f
wpa_gpg_data	7a e9 1c 87 1c 60 a7 10 5e 4e f6 87 bd 07 35 8f 26 ba 21 b5 5f d8 49 89 78 d3

Table 5. *Example of 3/4 message, protocol WPA-GPG.*

As already stated in section 1, in a significant scenario AP must also verify that the authenticating STA is authorized to do it.

3.4 Message 4/4

In WPA-PSK message 4 of 4 is a sort of acknowledgment sent by STA to AP, it contains nothing but a MIC. In WPA-GPG this message has fundamentally the same role, however, at this point in WPA-GPG STA still needs to derive PTK and needs to do some work:

- Decrypting the PMK;
- Deriving the PTK;
- Verifying message 3/4 MIC;

If MIC code verification is successful STA can send the last message and AP can authorize it to access the network. Actually at this point the Group-Handshake for GTK negotiation must be performed but we can skip the description of that protocol since nothing changes is WPA-GPG.

4 Conclusions

In this paper we introduced WPA-GPG, a modification on WPA-PSK authentication protocol that allows wireless authentication using GPG keys. Currently only the core of the authentication process is implemented and future development works will be done to allow the AP to verify that the provided key belongs to a specific key list (ACL style) or even to query a GPG key-server to check if the key has been signed by a trusted key (network of trust style). WPA-GPG does not require specific hardware nor firmware but works on WPA2 enabled wireless cards. WPA-GPG ensures the same level of security of WPA-PSK but it also guarantees in-network user privacy and non-repudiation of network traffic.

References

- [1] GNU. GnuPG. "<http://www.gnupg.org/>".
- [2] FON team. FON. "<http://www.fon.com/>".